REMARKS

In response to the Office Action of April 21, 2008, dependent claims 7 and 23 have been amended. Dependent claims 7 and 23 have been amended to correct for dependencies on claims that had been previously cancelled.

Claim Rejections- 35 U.S.C. § 103

At page 3 of the Office Action, claims 1-5, 7, 9-11, 17-21, 23, 25-26, and 31-35 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rindsberg (US Patent No. 6,970,565) in view of Herbert et al (US Patent No. 7,149,901, hereinafter Herbert) and Enichen et al (US Patent No., 6,333,983, hereinafter Enichen).

With respect to claims 1, 17, and 31-36, the Office asserts Rindsberg teaches a method of enhancing data security having actions corresponding to these claims, except for failing to specifically teach the generating of keys repeatedly and the use of strong and weak keys. The Office relies upon Herbert for teaching generating, in a secure execution environment of an electronic device to which access is restricted, a new secret key repeatedly and using the new secret key for encryption of files to be stored. The Office further relies upon Enichen for teaching receiving the strongly encrypted data, decrypting that data, and re-encrypting using less strong encryption. It is further asserted by the Office that it would have been obvious to a person of ordinary skill in the art to utilize Herbert's key generation method and Enichen's encryption method with Rindsberg's secure downloading system because it offers the advantage of increasing the strength of encryption by using multiple keys with smaller data samples (see Herbert, column 4, lines 40-46) and allowing for a faster decryption process due to the weaker key strength and allows for meeting export restrictions (see Enichen, column 1, lines 25-45). Applicant respectfully disagrees.

Enichen discloses a method for decrypting an input block encrypted under a predetermined key in a cryptographic system having a cryptographic facility providing cryptographic functions for transforming blocks of data. More particularly, these

functions include an encryption function for encrypting a block under a predetermined key and a transformation function for transforming a block encrypted under a first key to the same block encrypted under a second key (Enichen, Abstract).

In claim 1 of the present invention, in the secure execution environment, program code read from an external source where such program code is strongly encrypted is verified in the secure execution environment. The verified code is then encrypted with a less strong key and this less strongly encrypted program code is written into storage (memory). This set of actions is repeated; that is, the data is verified and a less strong new secret key is again generated, the data is encrypted with the less strong new secret key, and stored in the memory on a repeating basis. Such less strongly encrypted program code can be executed by a processor and the secure execution environment at a sufficiently rapid rate so that the overall appliance performs its intended functions in a timely fashion (Application as filed, page 6, lines 8-12).

It is asserted by the Office that it would have been obvious to utilize the method of Enichen to arrive at the method of claim 1 because it "allows for a faster decryption process due to the weaker key strength," with reference to column 1, lines 25-45. However, in this passage of Enichen, it is taught that the method and apparatus of Enichen solve the problem of meeting the Secure Electronic Transaction (SET) Protocol standards, which require use of Data Encryption Standard (DES) encryption and decryption with an 8-byte DES encryption key securely on a machine which does not have 56-bit DES enabled for software use (such as where DES with only 40 bit encryption keys is allowed due to US export regulations). The solution provided by Enichen to the problem relies on a transformation function, which is arranged to transform 56-bit DES encryption to 8-byte DES encryption by an encryption and a decryption process that makes use of hardware cryptographic primitive operations which do not require that strong encryption be enabled. Thus, a faster decryption process is neither the aim nor the result in Enichen.

The Office's reliance on column 12, lines 14-24 with respect to Enichen teaching receiving strongly encrypted data, decrypting that data and re-encrypting using less strong encryption, makes specific reference to column 12, lines 14-24 which in turn is referring to Figure 15. Figure 15 is described as showing data transformations involved in a procedure for decrypting a particular ciphertext data block. The fact that a "weak key" is mentioned in the cited passage does not in and of itself suggest the present invention since the overall processes as shown in the flow charts of Figures 11-19 involve concatenation of keys in order to allow for transformation of blocks of data using such keys so as to generate ciphertext or cleartext as generally discussed concerning the Data Encryption Standard (DES) at column 3, line 14 through column 4, line 61. There is no mention or suggestion in the cited passage or elsewhere in Enichen of generating in a secure execution environment a new secret key for less strongly encrypting verified data and writing this less strongly encrypted data into storage and repeating this process; thereby enabling the less strongly encrypted data to be more readily processing than the strongly encrypted data.

As mentioned above, the overall purpose of Enichen is to provide both an encryption and a decryption process that makes use of hardware cryptographic primitive operations which do not require strong encryption to be enabled thereby allowing for Secure Electronic Transaction (SET) protocol to be utilized even when encryption keys longer than 40 bits for data encryption/decryption are not allowed on a particular computing machine due to US export regulations.

Therefore, it is not seen why a person skilled in the art would be motivated to utilize a method according to Enichen in order to re-encrypt, in a secure execution environment, previously strongly encrypted data with a less strong encryption and to rely on the security of the environment itself, rather than on the strong encryption of the data, to provide a secure execution of the data within the secure environment. The use of a "weak key" in Enichen is part of a much more involved concatenation of keys which is different from the methodology of the present invention.

Because it would not be obvious to combine the references cited to arrive at the claimed invention, it is respectfully submitted that independent claims 1, 17 and 36 are not unpatentable over Rindsberg in view of Herbert and Enichen.

Since each of the independent claims of the present application is believed to be distinguished over the cited art, it is respectfully submitted that claims 2, 3, 5-16, 18, 19, and 21-35 are further distinguished over the cited art at least in view of such dependency.

Furthermore, at section 7 of the Official Action, the Office asserts with respect to claims 2 and 18 that Rindsberg as modified in view of Herbert (column 4, lines 20-30) teaches that a new secret key is generated when the device is booted. Applicant respectfully disagrees. This passage in Herbert describes the steps for installing a program in the secure system. It does not mention or suggest anything about booting as specifically required by dependent claims 2 and 18.

Furthermore, there is no discussion in this rejection of claims 2 and 18 of the previous amendment to claims 2 and 18 (in the Amendment After Final Accompanying RCE) wherein the word "initially" was added concerning the generation of a secret key being initially generated when the device is booted. Nowhere in the cited art is this feature of the present invention as claimed disclosed or suggested and for these reasons as well, dependent claims 2 and 18 are believed to be further distinguished over the cited art.

In view of the foregoing, it is respectfully submitted that the present application as amended is in condition for allowance and such action is earnestly solicited.

The undersigned respectfully submits that no fee is due for filing this Amendment. The Commissioner is hereby authorized to charge to deposit account 23-0442 any fee deficiency required to submit this paper.

Respectfully submitted,

Dated: July 18, 2008

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955

Alfred A. Fressola
Attorney for Applicant
Registration No. 27,550